

Data Protection Policy

Little Bowden Primary School



Please follow the Covid Risk Assessment when applying this Policy

Approved by: Governors

Date: 28/02/22

Last reviewed on: 28/02/2022

Next review due by: 28/02/2024

Contents

1. Aims.....	3
2. Legislation and guidance.....	3
3. Definitions	3
4. The data controller	4
5. Roles and responsibilities.....	4
6. Data protection principles.....	5
7. Collecting personal data.....	5
8. Sharing personal data	5
9. Subject access requests and other rights of individuals	6
10. Parental requests to see the educational record	7
11. CCTV	7
12. Photographs and videos.....	8
13. Data protection by design and default	8
14. Data security and storage of records.....	8
15. Disposal of records	9
16. Personal data breaches	9
17. Training.....	9
18. Monitoring arrangements	9
19. Complaints and the Information Commissioner Office (ICO)	9
20. Links with other policies	9
Appendix 1: Personal Data Breach Procedure	10
Appendix 2: Data Breach Flowchart.....	12
Appendix 3: Data Breach Form	13

.....

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK [General Data Protection Regulation \(UK GDPR\)](#) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the DPA 2018 and was brought into line with changes to the UK leaving the EU on 31st December 2020. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK [GDPR](#) and the ICO's [code of practice for subject access requests](#).

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none">• Racial or ethnic origin• Political opinions• Religious or philosophical beliefs• Trade union membership• Genetics• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes• Health – physical or mental• Sex life or sexual orientation
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Data subject	<p>The identified or identifiable individual whose personal data is held or processed.</p>
Data controller	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>

Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with UK GDPR and the Data Protection Act 2018, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is: Mr J A Walker,

Office7, The Courtyard
Gaulby Lane, Stoughton
Leicester, LE2 2FL

E: john@jawalker.co.uk T: 03337 729763

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals

- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, we will obtain parental consent for processing (except for online counselling and preventive services).

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's disposal schedule.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so within the limits of UK GDPR where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with, UK GDPR and DPA 2018.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification

- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Mr C Scrase, Premises Manager

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Child Protection Policy for more information on our use of photographs and videos.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our acceptable use policy)

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

19. Complaints and the Information Commissioner Office (ICO)

The school Complaint policy deals with complaints about Data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility or safeguarding and enforcing the DPA obligations.

E: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Acceptable use policy
- ICT Policy
- Child Protection and Safeguarding Policy

Appendix 1: Personal Data Breach Procedure

Data Protection Breach & Non-Compliance Procedure

All staff, governors and trustees must be aware of what to do in the event of a DPA / UK GDPR breach. The 'Data Breach Flowchart' outlines the process.

The 'Data Breach Form' must be completed and updated as the process progresses.

Most breaches, aside from cyber-attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Everyone needs to understand that if a breach occurs it must be swiftly reported. Examples of breaches are:

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar
- Sending an email with personal data to the wrong person
- Dropping or leaving documents containing personal data in a public place
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to school buildings or computer systems
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What to do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the Data Controller, Data Protection Compliance Manager and DPO as soon as possible, this is essential.

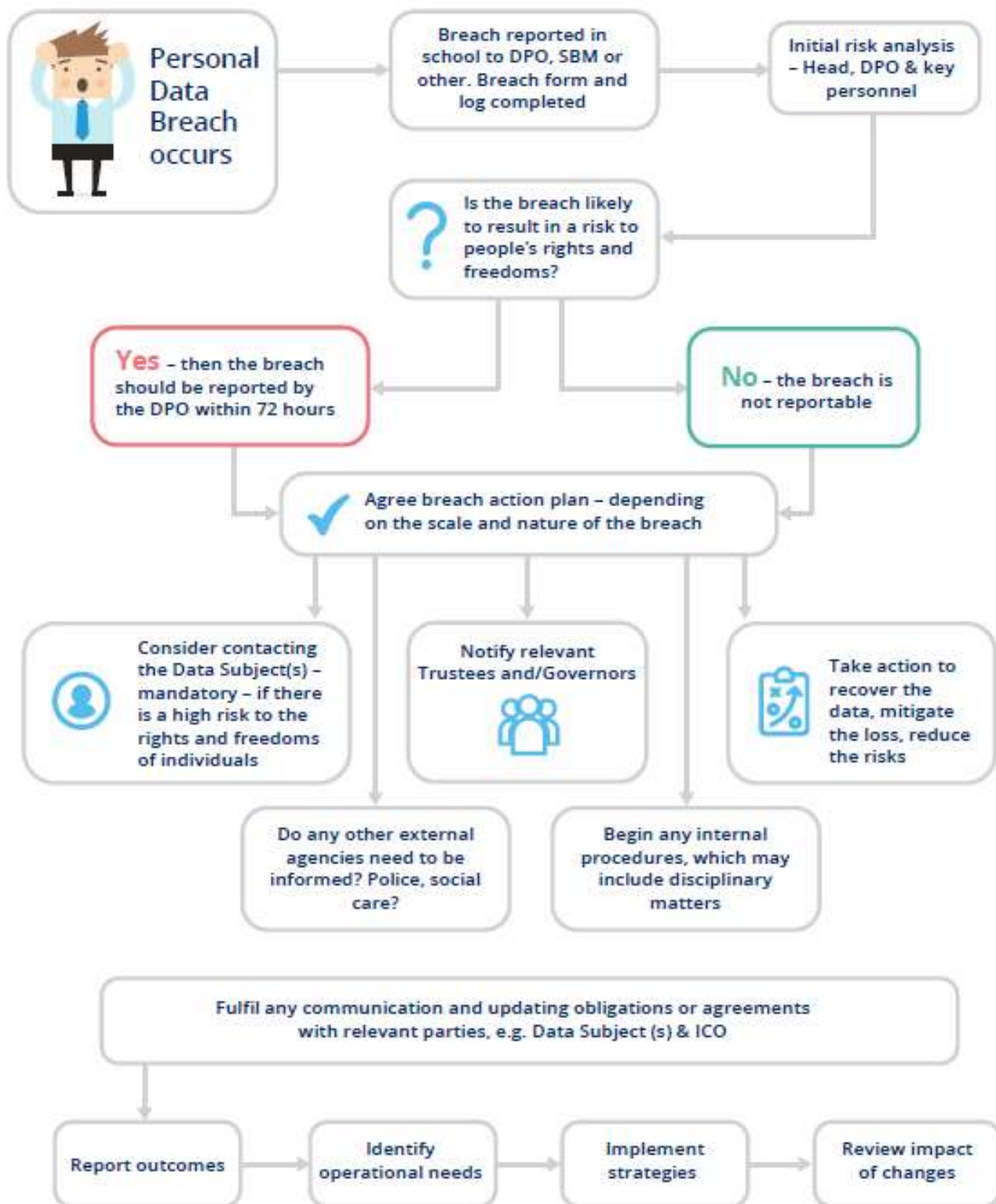
The breach notification form will be completed and the breach register updated.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.

The breach report will be within 72 hours of becoming aware of the breach.

It may not be possible to investigate the breach fully within the 72 hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

Appendix 2: Data Breach Flowchart



Appendix 3: Data Breach Form

School	
Date	
Reporter name and role	

Part A: Breach Information

When did the breach occur (or become known)?	
Description of Breach. This must include the type of information that was lost, e.g. name, address, medical information, NI numbers	
Which staff member was involved in the breach?	
Has the staff member had Data Protection Training within the last 2 years?	
Who was the breach reported to?	
When was the DPO notified?	
Date Reported:	
Time Reported:	
Initial Actions:	

Part B: Breach Risk Assessment

What type of data is involved:	Hard Copy: Electronic Data:
Is the data categorised as 'sensitive' within one of the following categories:	Racial or ethnic origin: Political opinions: Religious or philosophical beliefs: Trade union membership: Data concerning health or sex life and sexual orientation: Genetic data: Biometric data:
How was the data secured originally?	
How did the breach occur?	
What information was disclosed?	
Whose data has been breached?	
What risks could this pose? Be specific about this situation. If the risk is minimal, explain why.	
Are there wider consequences for the data subjects or school to consider e.g. reputational, loss of confidence?	
How many people might be affected by the breach? Either directly or indirectly.	

Part C – Cyber Breaches

Is this a cyber breach?	Yes/No If 'No' move to Section D
Has the confidentiality, integrity and/or availability of the system been affected. If so which and why	
What is the impact on the organization?	
What is the expected recovery time?	
Are any other IT systems/providers affected? If so, who and how?	

Part D: Breach Notification

Is the breach to be reported to the ICO? With reasons for decision	Yes/No Reasons
Date ICO notified	
Time ICO notified	
Reported by	
Method used to notify ICO	
ICO Reference No.	
Governors' Notified? Yes or No – reasons for decision at this point	
Notes:	
Is the data subject to be notified? Yes / No with reasons	Yes/No Reasons
Date and method data subject notified	
Notified by	
Response	

Part E: Breach Action Plan

Has the data been recovered? Is it likely to be recovered? What steps were taken to recover the data?	Yes/No Reasons
Who has been involved in the data recovery/breach management process?	
Do any other agencies need to be involved? If so, why?(e.g. police and social care)	
What will be done to prevent another breach	
Any training needs identified? For individuals and for whole staff?	